Industrial Control System (ICS) Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites

Sponsored by AlertEnterprise

Industrial Control System (ICS) Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites

January 2014

A SANS Analyst Whitepaper

Written by Scott D. Swartz and Michael J. Assante

This paper is a part of the Industrial Control Systems (ICS) Security Kit that will be provided to SANS 2014 ICS Summit & Training attendees. The 9th Annual ICS/SCADA Security Summit & Training will take place in Orlando, Florida, and attendees will experience many new topics, engaging speakers as well as exciting bonus events taking place only at the summit. Multiple technical courses taught by top ICS experts take place March 12–16. The two-day Summit commences the evening of March 16th, and the Summit program runs March 17–18. All Summit and course attendees will receive the ICS Security Kit, which will include research, practices guides and security tools. For more event information and to register, please visit, www.sans.org/event/north-american-ics-scada-summit-2014.

Introduction

The original version of this paper was funded and published by the Department of Homeland Security.[1] We have decided to recompose and augment our initial paper due to the persistent number of electric substation break-ins, and a more recent and disturbing trend of break-ins where nothing appears to have been taken.

Problem Statement

Physical break-ins and other unauthorized entries into unmanned critical infrastructure locations have historically been viewed only as traditional property crimes. This is particularly true for electrical power substations, where the obvious trespass, theft or vandalism is often considered the sole motive of the intruders. However, the increased use of computer networks to monitor and control unmanned facilities remotely has also increased the possibility that these traditional physical crimes could be a means or a cover for less discernible cybercrimes.

For example, the physical breach of an electrical substation in order to steal materials or equipment could be just that—a simple case of burglary and theft of property. However, in this day and age, such an event could just as easily be a front—a distraction in order to draw the asset owner's attention and investigation away from the real, more insidious motive. What if the true underlying motive was to gain access to the systems and devices within the facility—a system intrusion to either conduct immediate malicious acts or to introduce unauthorized hardware or software, thereby establishing a cyberbeachhead from which to launch future attacks, conduct network reconnaissance, or simply collect and steal sensitive information?

There are literally thousands of high-capacity keystroke loggers and other network surveillance products readily available on today's open market. Keyloggers are standard features of many remote-access Trojans. They can be hardware- or software-based, wired or wireless, and extremely easy to use and difficult to detect. A widely-cited, January 20, 2011 article also discusses the possibility of exploiting systems via USB keyboard emulators.[2] Malicious use of emulators could pose an even greater threat than keyloggers because emulators could be used to initiate keystrokes instead of simply recording them.

This is not a theoretical discussion. Our growing understanding of the Stuxnet worm,[3] originally carried in on a USB stick, demonstrates the effectiveness of surreptitiously gaining physical access to private or isolated networks. Security professionals often employ such tactics when conducting sanctioned network penetration tests for corporate clients. Another timely article reported that an unmarked computer had been discovered running in a spare room of Iceland's Parliament.[4] It was seized by police, and its exact purpose has not yet been determined or revealed. However, the fact that it was an unauthorized device connected to their network and was devoid of fingerprints or identifying serial numbers suggests malicious intent.

---

[1] www.us-cert.gov/control_systems/ics-cert

[2] www.h-online.com/security/news/item/Hacking-with-USB-keyboard-emulators-1172612.html

[3] www.langner.com/en/2013/11/20/langner's-final-stuxnet-analysis-comes-with-surprises

[4] www.grapevine.is/News/ReadArticle/Mysterious-Spy-Computer-In-Parliament-Works-Differently-Than-Being-Reported-Tech-Expert-Says

Security Ideals

The plans and success of any malicious cyber actor depend heavily on their target's daily routine and complacency, and human nature's tendency to not look beyond the obvious. This paper addresses the problem of blended intrusions by suggesting a cybersecurity response to facility break-ins that critical asset security managers can use to determine whether cyber assets might have been targeted during the physical breach. The response includes a systematic and graduated series of actions or checks for evaluating the integrity of cyberbased equipment once you have discovered evidence of a physical breach. Again, these are only suggestions, and any actions should be carefully considered in light of operational reliability, procedures and particular safety policies of the owners and operators.

This paper is not an exhaustive examination of all issues and possible actions, nor does it prescribe a process or promote civilian investigation of criminal activities. Although it does offer a few helpful tips to avoid common evidentiary pitfalls, the paper is not intended to conflict with any official investigation requiring specific procedures for collection, analysis or preservation of evidence for criminal prosecution. Rigid state and federal rules of evidence can vary significantly from even the most prudent commercial practices and procedures. We further suggest that owners and operators of critical infrastructures establish dialogue with their respective law enforcement agencies to discuss and resolve any conflicts between plans and procedures before such incidents actually occur.

We do encourage focused interactions between an organization's physical security and field engineering personnel and those responsible for the cybersecurity program. With these groups working together, organizations are better positioned to anticipate, investigate and respond to the growing occurrence of blended security threats.

Scenario

The following actions, checks and other suggestions could apply to virtually all industrial and critical infrastructure facilities and are especially useful to remote, unmanned facilities where conventional IT and/or industrial control systems are deployed. However, for simplicity, our scenario deals exclusively with a physical security breach of an unmanned electrical power substation. In this scenario, a break-in has been discovered and an investigation is underway by the owner/operator according to existing corporate policies and procedures. An inventory and damage assessment is being carefully conducted so as not to contaminate the scene and/or damage evidence in the event that local law enforcement is called in to conduct a formal criminal investigation.

Indications of a physical security breach may include, but are not limited to:

- Unreconciled door and/or cabinet alarms
- Unauthorized personnel or vehicles recorded by substation video camera (if installed)
- Damage or other signs of tampering to door locks or outside barrier fences
- Information from adjacent home or property owners
- Telltale evidence of vehicles or persons in and around the fence (tracks in the dirt or snow, or impressions found in the gravel typically used in substations)
- Inexplicable loss or behavior of communications links
- Inexplicable behavior of control system devices
- Missing or unaccountable items

Those investigating a physical security breach should at least consider the possibility that a cyberrelated incident may also have occurred. If the investigation of a physical security incident reveals that cyber or other electronic assets may have been disturbed or impacted, the actions in the following sections may be performed in response. Electrical substations are operational assets with economic, regulatory and safety consequences. Unauthorized changes to a control system's configuration or software have the potential to significantly impact reliable operations, asset availability and safety, thus producing a potential risk to equipment, operations and overall reliability.

Assumptions

When a physical security breach occurs at an electrical substation, the asset owner needs to validate the presence and integrity of all cyber assets. The extent of the investigation depends on indicators observed by the asset owner in and around the area where the physical breach occurred. The scenario and suggested actions presume the following:

- Network connectivity exists inside the substation or between another substation/control center and the affected substation.
- Modern electronic devices with the capability to obtain, store or transmit electronic data exist in or around the electrical substation.
- Devices and infrastructure that perform communications, control and network functions exist at the substation. Such items include, but are not limited to: PSTN lines, copper, fiber and RF devices; modems and communications processors; Ethernet switches; Remote Terminal Units (RTUs); relays; Programmable Logic Controllers (PLCs); other Intelligent Electronic Devices (IEDs) and so on.
- A *cybersecurity breach* is considered as any unauthorized access and/or change to a control system, unauthorized hardware or software placed onto a control system or network, an unauthorized physical connection to a control system network, and other similar situations.

Response

A systematic series of checks can be conducted to help determine whether or not sufficient evidence exists to indicate that a cybersecurity breach may have occurred in conjunction with the physical breach. Escalating levels of examination based on increasing indicators of a possible cyberbreach provide the decisional framework for balancing the need to gather system information against the risk or impact to operations in doing so. Conversely, you might also consider the risks to systems and operations in choosing not to conduct deeper evaluations that would have otherwise discovered a cyberbreach.

Escalating the Investigation

In this paper we cover three levels of examination: the initial examination, systems and configurations checks, and, if necessary, a detailed examination of file systems and binaries. Each level of escalation is necessarily more invasive and requires greater expertise and closer coordination with facility or company personnel responsible for corporate cybersecurity and production operations. Thus, management needs to be able to assess and balance the risks of escalation with the potential for outages and equipment and personnel safety caused by a cybersecurity breach of a critical asset. As the cyber investigation escalates, it is likely that any significant tests on control components may require specific test plans, procedures and perhaps even scheduled outages to obtain necessary information. The latter, of course, would be a worst-case scenario, and would be based on significant indications that a cyberbreach had actually occurred.

That said, before you examine cyber assets, an individual familiar with the site's physical configuration should examine the site for anything that appears missing or out of place. (This practice is usually referred to as a "yard or station walk down.") A staff member who is familiar with the facility's control devices should also be present and available to assist in the examination. It is important to log all observations. Photographic or digital video records of the scene can also be of great value because observations deemed insignificant during the initial discovery can sometimes prove otherwise later in the investigation. Again, take care not to disturb evidence the asset owner will need if the decision is made to involve the local law enforcement agency.

Absent emergency or other exigent circumstances, the following items are a short list of high-impact, on-scene physical do's and don'ts that could literally make or break your criminal case should it come to that.

- **Do** keep the number of initial employees entering the area to a bare minimum.
- Although it is recognized that the grounds of most substations are graveled, there are exceptions (for example, snow cover). Similar to fingerprints, the individual nature and unique blemishes of tire and footwear tread patterns can have significant evidentiary value. If tire tracks or footprints of potential suspects are present, **don't** trample over them! Where possible, maintain a discrete distance and follow your own tracks in and out of the location. You'd be surprised at the number of burglaries that are solved by the simple, yet compelling, forensic evidence these types of prints can provide. In fact, such prints are so vital to criminal investigations that if there is a risk of losing them to the elements—wind, snow, rain, sun—**do** consider covering some of the better impressions with a few carefully placed cardboard boxes, open ends down so as not to disturb the print.

- With regard to footprints, if you suspect that the control house has been entered, **do** be mindful of where you step. The same basic rules apply, but with an additional twist. First, **do** keep personnel numbers to a bare minimum. If possible, **do** stay close to the walls, avoiding normally traveled pathways. Most control house floors present a relatively smooth surface, so that even if you cannot visually detect footprints, for example muddy or other visible indicators, it does not mean none exist. You just can't see them. The floor could appear clean and absent of any evidence at first glance; however, it likely holds a wealth of potential evidence should you decide to engage law enforcement. An effective collection technique used by criminal investigators is to extinguish the interior lighting and then run a flashlight close and parallel to the floor. The floor's surface will come alive with clear, distinct prints in the dust. Those that appear to be "on top" of all the others most likely belong to the suspects. A few close-in shots of no-flash photography using the side lighting provided by the flashlight, and the evidence is preserved for later comparisons against potential suspect's footwear.
- Again, absent emergency or other exigent circumstances, **don't** handle or otherwise disturb potential physical evidence until you've had the opportunity to fully complete the initial walk down and determine whether or not to engage law enforcement! Perhaps take a picture, note the date and time, but leave the actual handling to the proper authorities. Keep your hands in your pockets—just as you instruct escorted substation visitors! It's a bit embarrassing to learn that all the usable prints lifted off a piece of evidence are actually staff's—simply because they couldn't resist the urge to paw the scene.

Finally, should on-scene observations and other indicators heighten suspicions of a possible cybersecurity breach, your investigation should escalate accordingly. Efforts may soon shift from the gathering and preservation of physical evidence to gathering and preserving electronic evidence. At this point, the necessary methods and skill sets to properly do so will become important factors. Escalation beyond initial visual and cursory examinations usually requires skills and expertise commensurate with that required for hardware and software installations, upgrades or restoration of service of control equipment by the appropriate vendors, consultants or in-house technicians. Management should also determine if it is necessary to pursue additional forensic analysis in support of law enforcement investigations and to identify and direct appropriate expertise in providing that support.

The following checks are only suggestions and should be modified and implemented in line with the particular facility's systems, cyber assets and operational construct.

1. Initial Examination

The first step is to examine items that can be checked visually. The use of photography (preferably digital) with an accurate date and time stamp is important for documenting potential evidence. Visual examinations of cyber assets typically include such things as these:

- Looking for signs of entry into the building or cabinets where cyber assets are stored. This could include footprints or disturbed items inside and outside the building.
- Looking for evidence of tampering with all cyber assets—for example, disturbed dust or dust texture and composition inconsistent with that around it, broken tamper seals or other signs that a rack or case has been opened.
- Inspecting physical connections to all cyber assets for signs of tampering.
- Checking front panel indicator lights for proper illumination. Compare indicators to station checks (normal illumination) because tampering may have triggered visual indicators.
- Checking for missing, unfamiliar or new hardware or media located in and around the substation, as well as communications equipment that might be outside the perimeter. Examples include USB or PS/2 devices, covert wireless cards or access points or keyboards. (See Appendix A for several examples of readily available covert devices.)
- Checking with the control center to see if any unusual alarms, events or logs appeared on the control system or if there were any interruptions in connectivity or service during the timeframe associated with the physical intrusion.
- Analyzing the physical breach to determine a motive and correlate it to any cyber information or devices. Does the physical breach resemble any other recent intrusions at other facilities?
- Locating communication links and terminations to the substation, including third-party equipment inside or outside the physical perimeter, and determining whether they have been tampered with.
- Looking for signs of a search for documents. Passwords are frequently posted on the undersides of keyboards, behind monitors, inside drawers and cabinet doors and so on. An intruder who is looking for quick cyber access will likely search for any information that can be helpful and, in doing so, may have disturbed keyboards or other devices.
- Using a WiFi sniffer or RF signal detector, if possible, to scan for suspicious or unauthorized emanations. These types of tools are readily available and easy to use, and they should be considered as part of routine inspections as well as in response to physical breaches.

If any evidence of a potential cybersecurity breach is discovered during the initial inspections, the asset owner might consider engaging appropriate law enforcement authorities at this point to ensure proper follow-on actions, evidence collection requirements and so on. In any case, the following are offered as generic guides for additional investigation of cybersecurity breaches.

2. Systems and Configurations Check

A systems and configurations check examines control system components, often through the use of an engineering workstation or laptop computer. We recommend that the computer used for this purpose should not have been connected to the affected cybernetwork or devices. An individual who is experienced with conducting forensics examinations of cybersystems should work with the responsible control system engineers or field personnel to perform the remainder of the investigation. This will help ensure data integrity and adherence to proper rules of evidence.

In accordance with the particular facility's systems, cyber assets and operational construct, examining the control system components may include the following items:

- Logging into each cyberdevice using the engineering workstation or laptop and checking the log history to see whether any recent unauthorized configuration changes occurred and whether any recent changes occurred in the date/time of files applicable to cyberdevices
- Logging into each network device using the engineering workstation or laptop and checking for proper functionality and network connectivity, as well as any suspicious network connections
- Checking each device for uptime or any other signs of the device being restarted
- Looking for new user accounts, new group settings, hidden files, new or modified directories or drive partitions, changed passwords, newly installed software, system files that have been tampered with, or changes to the operating system of the device
- Examining perimeter networking and security devices such as firewalls, routers, and network intrusion detection systems for any signs of unusual network activity
- Checking any removable media drives or ports for unrecognized media or devices the intruder may have left behind
- Verifying the configuration of each device against your configuration management records and carefully noting and following up on any deviations from the documented configuration

3. File System and Binary Examination

Forensics is considered a secondary priority to system operation and restoration. However, digital forensics can provide important information regarding the methods, sources and extent of the compromise that may not otherwise be available. Wherever possible and practical, consider capturing an image of the systems or devices prior to manipulation. This is important regardless of whether or not you will pursue criminal prosecution.

A file system and binary examination of each cyberdevice confirms whether files are clean and uncorrupted, whether proper configurations are loaded onto each device, and whether network services are correctly configured and operating properly. Performing a file system and binary examination may include the following:

- Checking the timestamps of configuration files and the size of system binaries against trusted binaries. If there is suspicion that some files may be corrupted, modified or contain malware, work with the control center and field engineers to determine whether the device can be disconnected to minimize any opportunities for propagation.
- Checking the firmware of any upgradable devices for evidence of recent changes.
- Scanning applicable cyberdevices using the engineering workstation or laptop and looking for viruses, malware or Trojans. This check may be performed if the system has been tested and is capable of scanning without impacting critical applications or the local networked devices.
- Obtaining configuration managed files (from a trusted source) and reloading configurations to each cyberdevice. Be sure to wipe previous configurations of each cyberdevice clean.
- Having the communications provider perform both a physical and network check of the communication network.

If there is any evidence of cyber intrusion, it is best to reimage the system—if such images are maintained. As an alternative, perform a clean reinstallation of the operating system and all required software from a trusted source for all affected components. If applicable, delete, recreate and reformat all hard drive partitions prior to reinstalling the clean operating system and applications.

Conclusion

The benefits realized through increased use of complex technologies and network convergence also provide new and often unrecognized attack vectors for malicious actors. The proliferation of digital devices and expansion of interconnected networks combined with the sophistication of malicious tools, as demonstrated by the Stuxnet worm, requires a holistic response to discovered security events or incidents. The cybersecurity response to physical security breaches described in this paper has been provided as an approach for security managers to consider when assessing the impact of physical intrusions of field sites containing intelligent electronic devices. This is certainly effective for critical cyber assets or cyber assets that otherwise fall within the electronic security perimeter, but it should be extended to any susceptible field location. The prescribed actions are primarily intended to motivate critical asset owners to consider whether a cybersecurity breach has taken place. The procedures, however, should only be considered in light of operational, safety and maintenance environments created by the particular asset owner to meet required business and regulatory requirements.

Physical evidence of intrusion into control systems cabinets, communications and networks, and intelligent control devices or terminals should be a serious indicator that the integrity of these devices is suspect and that the systems they control could be at risk. The owners and operators of critical cyber assets should review their current policies and practices for responding to physical security breaches to ensure they also address and verify cybersystems integrity. Such response plans should also include steps for reporting intrusions to the Electric Sector - Information and Analysis Sharing Center (ES-ISAC), the Department of Energy through the OE-417 reporting form and/or to the DHS Industrial Control Systems Computer Emergency Response Team (ICS-CERT).

Although the electric utility sector is the critical infrastructure referred to in this paper, all industry sectors (gas, oil, transportation, water and so on) that have remote, unmanned sites with control system cyber assets can benefit from increased awareness in responding to the possibility of a cybersecurity breach coincident to a physical security breach.

ICS-Cert Assistance Points of Contacts

Contact the Department of Homeland Security (DHS) ICS-CERT to report and address information technology and industrial control systems security issues.

Requests for assistance from ICS-CERT can be made by contacting the organization directly via telephone at 877-776-7585 or by sending an email to ics-cert@dhs.gov. Information about the ICS-CERT can be found on their website at **www.us-cert.gov/control_systems/ics-cert**.

Appendix A

The following images depict just a few of the many covert hardware devices used to compromise and exploit cyber assets and information.

USB keyloggers

PS/2 Keyloggers

Wireless Keyloggers

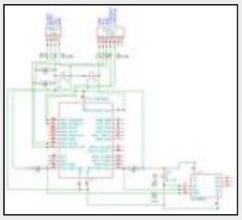
I/O Card Keyloggers

Keyboard keyloggers

Keyboard Emulators

Video loggers

Miscellaneous



About the Authors

Scott D. Swartz is a retired cybersecurity professional and former Energy Infrastructure and Cyber Security Advisor for the Federal Energy Regulatory Commission (FERC), where he provided guidance to the Commission and senior staff on physical and cybersecurity issues affecting the nation's bulk power system. Prior to working for the FERC, he developed and implemented a control systems security program for the Department of Defense (DOD), Mission Assurance Division. Before his DOD experience, he conducted field disaster response and recovery operations for the Federal Emergency Management Agency and was later recruited into their Office of Cyber Security. Mr. Swartz entered federal service with 16 years of law enforcement experience including patrol, investigations and special operations. He holds Bachelor of Science degree in business administration and industrial technology and a Juris Doctor from the University of North Dakota, where he also taught a 300-level undergraduate course in criminal law and procedure.

Michael Assante is currently the SANS lead for training on Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) security. Mr. Assante was most recently chief executive officer of NBISE and Chair of NBISE's national board. He previously held the position of vice president and chief security officer at the North American Electric Reliability Corporation (NERC) and oversaw the implementation of cybersecurity standards across the North American electric power industry. Prior to joining NERC, Michael held notable positions at Idaho National Labs, was vice president and chief security officer for American Electric Power, and pioneered the security intelligence landscape in his role as chief operating officer of LogiKeep. A former U.S. Navy intelligence officer with experience in information warfare and information security management, Mr. Assante recognized the need to bring intelligence-type analysis to the networks of the corporate world by identifying risks and threats specific to the hardware, software and systems used by individual organizations.

SANS would like to thank its sponsor:

AlertEnterprise!

Last Updated: March 31st, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS New Orleans 2020	**New Orleans, LAUS**	**Jun 08, 2020 - Jun 13, 2020**	**Live Event**
SANS Las Vegas Summer 2020	**Las Vegas, NVUS**	**Jun 08, 2020 - Jun 13, 2020**	**Live Event**
SANSFIRE 2020	**Washington, DCUS**	**Jun 13, 2020 - Jun 20, 2020**	**Live Event**
SANS Chennai 2020	**Chennai, IN**	**Jun 22, 2020 - Jun 27, 2020**	**Live Event**
SANS Pittsburgh 2020	**Pittsburgh, PAUS**	**Jun 22, 2020 - Jun 27, 2020**	**Live Event**
SANS Silicon Valley - Cupertino 2020	**Cupertino, CAUS**	**Jun 22, 2020 - Jun 27, 2020**	**Live Event**
SANS Cyber Defence Canberra 2020	**Canberra, AU**	**Jun 29, 2020 - Jul 11, 2020**	**Live Event**
Cyber Defence Japan 2020	**Tokyo, JP**	**Jun 29, 2020 - Jul 11, 2020**	**Live Event**
SANS Perth 2020	**Perth, AU**	**Jun 29, 2020 - Jul 03, 2020**	**Live Event**
SANS Chicago Spring 2020	**OnlineILUS**	**Jun 01, 2020 - Jun 06, 2020**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**